7 DAY CYBER LOCKDOWN PLAN

EXECUTIVE CYBER RISK REDUCTION FRAMEWORK FOR SMALL BUSINESS LEADERS

SERIAL ENTREPRENUR

BY Vernon Tryon

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

7-Day Cyber Lockdown Plan

Executive Cyber Risk Reduction Framework
for Small Business Leaders

Prepared by
Small Business Services IVT LLC

5425 N 103rd St, Suite 4
Omaha, NE 68134

Author
Vernon Tryon

Executive Brief

Cybersecurity is no longer just an IT responsibility.

It is a leadership responsibility that directly impacts revenue protection, client trust, regulatory exposure, and operational continuity.

Small businesses and tax professionals are increasingly targeted because attackers view them as high-value, low-resistance environments. Organizations often maintain large amounts of financial and personal data while operating without dedicated security teams.

The purpose of this guide is to provide a practical executive framework that helps business owners reduce preventable cyber risk within seven structured working sessions.

Each section focuses on leadership decisions and operational safeguards rather than complex technical procedures.

By implementing the steps outlined in this plan, business leaders can significantly reduce common vulnerabilities that lead to costly cyber incidents.

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

Table of Contents

How to Use This Plan

This plan is designed to be implemented with over seven focused working sessions.

Each day requires approximately 30–60 minutes of leadership review and execution.

You may involve your office manager, operations manager, IT provider, or technology support partner when necessary. However, the actions outlined in this framework are designed so that business leadership can initiate the process without requiring deep technical expertise.

Each section includes:

• Strategic Objective
• Why It Matters
• Leadership Action Steps
• Executive Verification Checklist

Completion of all seven sections creates a stronger operational cybersecurity foundation.

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 1 — Secure Executive and Operational Email Systems

Strategic Objective

Secure your organization's primary communication channel and reduce the most common entry point for cyber-attacks.

Why This Matters

More than eighty percent of cyber breaches begin with email compromise, phishing attempts, or unauthorized mailbox access.

Because email accounts often connect to financial software, client communications, and cloud systems, compromising a single mailbox can expose the entire business.

Leadership Actions

1. Enable multi-factor authentication for all company email accounts.
2. Review all administrative email accounts and remove unnecessary privileges.
3. Disable automatic email forwarding to unknown external addresses.
4. Remove inactive or unused mailboxes.
5. Confirm spam and malware filtering protections are active.

Executive Verification Checklist

☐ Multi-factor authentication enabled for all accounts
☐ Administrative accounts reviewed
☐ Email forwarding rules verified
☐ Unused accounts removed
☐ Email security filtering active

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 2 — Enforce Access Control and Credential Governance

Strategic Objective

Strengthen authentication controls and eliminate weak credential practices.

Why This Matters

Weak passwords, shared credentials, and uncontrolled system access represent one of the most common causes of unauthorized entry into business systems.

Strong credential governance significantly reduces this exposure.

Leadership Actions

1. Implement a password manager for company accounts.
2. Require strong passwords with a minimum of fourteen characters.
3. Eliminate shared login credentials.
4. Review administrative access privileges.
5. Apply multi-factor authentication to financial systems.

Executive Verification Checklist

☐ Password manager implemented
☐ Password policy established
☐ Shared credentials removed
☐ Administrative access reviewed
☐ Financial system MFA enabled

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 3 — Protect Client and Financial Data

Strategic Objective

Safeguard sensitive business and client data from unauthorized access.

Why This Matters

Tax professionals, consultants, and service businesses frequently store financial data, personal records, and client documentation that attackers can exploit.

Protecting this data is essential for maintaining client trust and regulatory compliance.

Leadership Actions

1. Identify all locations where client data is stored.
2. Encrypt laptops and company devices.
3. Restrict access to sensitive folders and records.
4. Review cloud storage permissions.
5. Verify vendor and third-party access rights.

Executive Verification Checklist

☐ Data storage locations identified
☐ Devices encrypted
☐ Folder access restricted
☐ Cloud permissions reviewed
☐ Vendor access verified

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 4 — Reduce Phishing and Social Engineering Risk

Strategic Objective

Strengthening employee awareness and reduce exposure to deceptive communications.

Why This Matters

Phishing remains the most common method attackers use to gain access to business systems.

Employees who understand the warning signs of suspicious messages can stop attacks before they begin.

Leadership Actions

1. Inform employees about current phishing threats.
2. Enable email warning banners for external senders.
3. Block executable email attachments.
4. Disable automatic macro execution in office documents.
5. Establish a process for reporting suspicious emails.

Executive Verification Checklist

☐ Phishing awareness reminder sent
☐ External email warnings enabled
☐ Dangerous attachments blocked
☐ Macro settings restricted
☐ Reporting procedure documented

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 5 — Establish Reliable Data Backup and Continuity

Strategic Objective

Ensure the business can recover from ransomware or system failure.

Why This Matters

Businesses that maintain reliable backups can restore operations quickly after a cyber incident.

Without verified backups, ransomware attacks can halt operations indefinitely.

Leadership Actions

1. Confirm automated daily backups are running.
2. Maintain at least one offline or immutable backup copy.
3. Test file restoration procedures.
4. Confirm accounting and financial systems are included in backups.
5. Document backup provides contacts information.

Executive Verification Checklist

☐ Daily backups confirmed
☐ Offline backup copy verified
☐ Restoration test completed
☐ Financial systems included
☐ Vendor contacts documented

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 6 — Reduce Employee and Operational Risk

Strategic Objective

Limit internal access exposure and reduce operational vulnerabilities.

Why This Matters

Employee access, outdated permissions, and uncontrolled technology usage can unintentionally create security gaps.

Managing internal access protects the organization from preventable risks.

Leadership Actions

1. Remove access for former employees.
2. Review permissions for current staff members.
3. Establish guidelines for AI tool usage.
4. Limit installation of unauthorized software.
5. Define minimum cybersecurity expectations.

Executive Verification Checklist

☐ Former employee accounts removed
☐ Staff access reviewed
☐ AI usage guidelines established
☐ Software installation controls applied
☐ Security expectations documented

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

DAY 7 — Create a Cyber Incident Response Plan

Strategic Objective

Prepare leadership to respond quickly and effectively to a cybersecurity event.

Why This Matters

Organizations that prepare response procedures in advance recover faster and limit financial damage.

A structured response plan ensures leadership knows exactly what steps to take if systems are compromised.

Leadership Actions

1. Identify the internal incident response lead.
2. Document cyber insurance information.
3. Create an internal communication chain.
4. Identify external legal or technical contacts.
5. Store emergency contacts offline.

Executive Verification Checklist

☐ Incident response lead identified
☐ Insurance details documented
☐ Communication plan defined
☐ External contacts listed
☐ Emergency information stored securely

Small Business Services IVT LLC
5425 N 103rd St, Suite 4
Omaha, NE 68134

Strategic Next Steps

Completing this **7-Day Cyber Lockdown Plan** establishes a stronger security baseline for your organization.

However, cybersecurity is not a one-time initiative.

Threats evolve constantly, and business leaders must stay informed about emerging risks that impact financial systems, tax data, and client information.

Small Business Services IVT LLC publishes the Small Business Cyber Brief, an executive-level cybersecurity intelligence newsletter designed for business owners and tax professionals.

Click Here For Cyber-Security Newsletter

Subscribers receive:

- Weekly threat briefings
  - Cyber risk insights for business leaders
  - Cyber Security Tips
  - Business Coaching Insights
- FREE How to eBook Each Month

To continue strengthening your cybersecurity posture, consider subscribing for ongoing strategic guidance.

Small Business Services IVT LLC
Cyber Risk Advisory and Business Protection Services

5425 N 103rd St Suite 4, Omaha NE 68134
